REMARKS

Claims 1, 5-6, 8-12, 16-17, 19-23, and 25-30 are pending in the Application and are now presented for examination. Claims 1, 10, 11, 12, 21, 22, 23 25 and 26 have been amended. No new matter has been added.

Claims 1, 10, 12, 21, 23, 25 and 26 are independent.

The claims relate to providing automated tracking of security vulnerabilities. In one embodiment, the method includes using a computing device to perform a security vulnerability assessment on a system and detecting the presence of a security vulnerability in the system. In response to detecting the presence of the security vulnerability, storing data obtained from the security vulnerability assessment in a security vulnerability database. Also, using a computer program, a security vulnerability score is determined. The security vulnerability score is based on a frequency score, a severity score, a criticality score, and a trust score. The frequency score is based on a percentage of hosts experiencing the detected security vulnerability in the system. The criticality score is based on whether at least one of confidential data and personal data is on the system and whether information on the element is itself used for aggregation. Also, a time to fix the security vulnerability detected by the security vulnerability assessment of the system is determined based on the determined security vulnerability score.

Allowed Claims

Claims 1, 5, 6, 9, 12, 16, 17, 19, 20, 23 and 27-30 are allowed (*See* Examiner's Answer dated March 3, 2009). Allowed Claims 1, 12 and 23 have been amended to more clearly recite what Applicants believe is the invention.

Patentability Under 35 U.S.C. § 112, Second Paragraph

On page 5 of the Board of Patent Appeals and Interferences (B.P.A.I.) Decision dated August 16, 2011 (hereinafter "B.P.A.I. Decision"), the rejection of Claims 11, 22 and 25 as allegedly being indefinite under 35 U.S.C. § 112, second paragraph, was affirmed. In particular, the B.P.A.I. Decision states that the claimed feature of "whether information on the element is used for aggregation" is directed to "at least two plausible claim constructions…(1) information on the element is used for aggregation if the at information describes how to perform the aggregation and (2) information is used for aggregation if that information itself is aggregated (i.e., is a component of an aggregation)" (Page 6 of the B.P.A.I. Decision). Applicants have amended Claims 11, 22 and 25 to address the rejection by removing reference to the aggregation feature.

As such, Applicants believe the amendments to Claims 11, 22 and 25 have overcome the 35 U.S.C. § 112, second paragraph rejection.

Accordingly, Applicants respectfully request the withdrawal of the rejection to Claims 11, 22 and 25.

Patentability Under 35 U.S.C. § 103

Page 4 of the B.P.A.I. Decision reversed the rejections of Claims 11, 22 and 25 under 35 U.S.C. § 103(a). As such, as discussed above with respect to the new grounds of rejection set out in the B.P.A.I. Decision, Applicants believe amended Claims 11, 22 and 25 are in condition for allowance.

The rejections of Claims 10, 21 and 26 under 35 U.S.C. § 103(a), were affirmed on page 7 of the B.P.A.I. Decision. On page 5 of the September 10, 2008 Final Office Action, Claims 10, 21 and 26 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over United States Patent No. 7,243,148, issued to Keir *et al.* ("Keir") in view of United States Patent No. 5,944,825, issued to Bellemore *et al.* ("Bellemore") in further view of United States Patent Publication No. 2004/0006704, to Dahlstrom *et al.* ("Dahlstrom"). Applicants have amended Claims 10, 21 and 26 to address the affirmed rejections.

In particular, amended Claims 10, 21 and 26 recite, in part, "determining a time, **based on the security vulnerability score**, to fix the security vulnerability" (emphasis added). Keir, Bellemore and Dahlstrom, whether considered individually or in combination, fail to disclose or suggest these features.

Page 3 of the Office Action states that "Keir fails to explicitly disclose determining a time to fix a security vulnerability identified by the security vulnerability assessment of the system based on the determined security vulnerability score." Applicants agree that Keir fails to disclose or suggest these features.

Bellemore merely describes that a "[p]lurality of fields 511 of the user profile table 207 contain data which represent thresholds associated with individual users or classes of users" (col. 5, lines 16-18). In particular, there is a "failed_login_attempts field represents a threshold number of attempts of using an invalid password…before temporarily locking the account" (col. 5, lines 18-21). For example, Bellemore temporarily locks the account "for a threshold period of time" if the threshold number of attempts are met (col. 6, lines 32-33). Temporarily locking of

the account is simply not directed at "**determining a time…to fix** the security vulnerability" let alone doing so using Applicants' determined security vulnerability score.

Moreover, Bellemore describes a "password_life_time field", "password_reuse_time field", "password_reuse_max field", "password_verify_function" field, "password_lock_time field", and "password_grace_time field" in which these fields are merely predefined "thresholds associated with individual users or classes of users" (col. 5, lines 16-34). For example, "[t]he password_reuse_time field represents the period of time in which the use of a password for a user ID can not be repeated" (col. 5, lines 23-26). "The password_grace_time field represents the period of time allotted to change a password after the password life time has been expired" (col. 5, lines 31-34). Bellemore's threshold fields are simply not used to determine "**a time…to fix** the security vulnerability" let alone doing so using Applicants' determined security vulnerability score as recited in Claims 10, 21 and 26. As such, Bellemore fails to disclose or suggest the features of Claims 10, 21 and 26.

Dahlstrom does not cure the deficiencies of Keir and Bellemore. Dahlstrom merely describes "a process for determining security vulnerabilities" that includes comparing product records (¶ [0043]; FIG. 5). For example, characteristics of each product are compared to a plurality of product records (Abstract). Each product record includes fixes associated with each security vulnerability (Abstract). Dahlstrom records that include fixes for each security vulnerability is simply not directed to determining "**a time…to fix** the security vulnerability" let alone doing so using Applicants' determined security vulnerability score as recited in Claims 10, 21 and 26. As such, Dahlstrom does not disclose or suggest the features of Claims 10, 21 and 26.

Accordingly, Keir, Bellemore and Dahlstrom, whether considered individually or in combination, fail to disclose or suggest the features of Claims 10, 21 and 26. Applicants respectfully request the withdrawal of the rejection to Claims 10, 21 and 26.

For all of the above reasons, the claim rejections are believed to have been overcome placing Claims 10, 11, 21, 22, 25 and 26 in condition for allowance (Claims 1, 5, 6, 9, 12, 16, 17, 19, 20, 23 and 27-30 are allowed), and reconsideration and allowance of thereof of the rejected claims is respectfully requested.

The Examiner is encouraged to telephone the undersigned to discuss any matter that would expedite allowance of the present application.

The Commissioner is hereby authorized to credit overpayments or charge payment of any additional fees associated with this communication to Deposit Account No: 090457.

Respectfully submitted,

Date: October 12, 2011

By: /Alan M. Weisberg/

Alan M. Weisberg
Reg. No.: 43,982
Attorney for Applicants
Christopher & Weisberg, P.A.
200 East Las Olas Boulevard, Suite 2040
Fort Lauderdale, Florida 33301
Customer No: 68786
Tel: (954) 828-1488
Fax: (954) 828-9122
email: ptomail@cwiplaw.com

317180